ABSTRACT

~~Method and Communications System for Ciphering Information for a Radio Transmission and for Authenticating of Subscribers~~

The subject matter of the invention proceeds from an encryption of the information for the radio transmission in an access network (ACN) as well as an authentication in at least one core network (CON1, CON2). Inventively, public keys (PUK1-MT, PUK-BS) are mutually transmitted between a mobile station (MT) and the base station (BS) via the radio interface (AI), and the public key (PUK1-MT or, ~~respectively,~~ PUK-BS) received by the base station (BS) or, ~~respectively,~~ mobile station (MT) is employed for the encryption of the information to be subsequently sent via the radio interface. On the basis of a private key (PRK1-MT, PRK1-BS) that is allocated to the transmitted, public key (PUK1-MT, PUK-BS) in the mobile station (MT) or, ~~respectively~~, in the base station (BS), the encrypted information received by the mobile station or, ~~respectively,~~ base station can be deciphered. Following the encryption procedure, a ~~mobile radio telephone-specific means (SIN)~~ subscriber identity mobile card (SIM) of the mobile station implements the authentication of the respective core network (CON1, CON2), and ~~a means~~ authentication equipment (AC, AC') of the core network implements the authentication of the subscriber on the basis of the mutually transmitted, encrypted information.

~~FIG. 1~~